SB 676 PERSONAL INFORMATION BREACH/NOTIFICATION FORM

Maryland Department of Health

Investigation and Risk Assessment

DETERMINING A PERSONAL INFORMATION BREACH:

Was there an unauthorized acquisition of Personal Information (PI) as the result of a computer incident? _____

_____

If yes, explain: _____

_____

_____

Does the computer incident also involve an impermissible acquisition, access, use or disclosure of Protected Health Information (PHI)? (Y or N) _____
If yes, complete this form and also adhere to the MDH HIPAA Breach Response Policy.

Does the computer incident involve any of the following exceptions to the definition of Personal Information? _____

_____

If yes, which one? _____

_____

1) Is publicly available information that is lawfully made available to the general public from federal, State, or local government records;

2) An individual has consented to have disseminated or listed;

3) Except for a medical record that a person is prohibited from re-disclosing under § 4-302(d) of the Health-General Article, is disclosed in accordance with the Health Insurance Portability and Accountability Act (HIPAA); or

4) Is disclosed in accordance with the Federal Educational Rights and Privacy Act (FERPA).

What type of Personal Information is involved in the computer incident? _____

_____

Who was the unauthorized person that acquired the Personal Information? _____

_____

What was the cause of the computer incident? _____

_____

What was the extent of the computer incident? _____

_____

Can the computer incident be contained? _____

_____

Was the Personal Information encrypted? _____
And if so, was the encryption key broken? _____

What type of harm could potentially be caused by the computer incident?_____

_____

_____

Will the unauthorized acquisition of the Personal Information of the individual(s) result
in or is likely to result in the misuse of the information? _____

_____

**DO YOU THINK THIS CONSTITUTES A SB 676 BREACH OF PERSONAL
INFORMATION UNDER THE MDH PERSONAL INFORMATION BREACH
RESPONSE POLICY? WHY OR WHY NOT?** (Explain your logic)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Notes: (anything else not covered)

_____
_____
_____
_____
_____

COMPLETE THE FOLLOWING WHERE APPLICABLE:

*Information about the Unit:

Name: _____

Address: _____

_____

Investigator:_____ Phone:_____

Email:_____

*Information about the Nonaffiliated Third-Party: (if applicable)

Name: _____

Address: _____

_____

Investigator: _____ Phone: _____

Email:_____

*Information regarding the Breach:

Date of Breach: _____ Date of discovery: _____

Approximate # of individuals affected? _____ 1000 or more? _____

Type of Breach: (e.g., unauthorized access, denial of service, malicious code, improper usage, improper destruction): _____

_____

Location of Breached Information: (e.g., laptop, desktop, email, network, data base)

_____

_____

Type of Personal Information involved: (e.g., demographic, financial, ID number) _____

_____

_____

Brief description of the Breach: _____

_____

_____

_____

_____

Types of safeguards that were in place prior to the Breach: (e.g., firewalls, encryptions, locks) _____

_____

_____

*Notice of Breach and Actions Taken:

Date(s) Notice was given to individual(s): _____

Was substitute notice required? (Y or N) _____

Was Media Notice required? (Y or N)_____ ___

Actions taken in response to the Breach: (e.g., mitigation, sanctions, safeguards, policies)
_____ ___
_____ ___
Describe the actions taken: _____ ___
_____ ___
_____ ___

* Required fields: These fields will be a part of the log that is maintained by the MDH Privacy Officer. Please make sure they are filled out as thoroughly and as accurately as possible.

_____   _____ ___
Name   Date

_____
Signature